

The CCM Validation System (CCMVS)

September 7, 2004

Lawrence E. Bassham III

National Institute of Standards and Technology

Information Technology Laboratory

Computer Security Division

TABLE OF CONTENTS

1	INTRODUCTION.....	1
2	SCOPE.....	1
3	CONFORMANCE.....	1
4	DEFINITIONS AND ABBREVIATIONS	1
4.1	DEFINITIONS.....	1
4.2	ABBREVIATIONS	2
5	DESIGN PHILOSOPHY OF CCM VALIDATION SYSTEM.....	2
6	CCMVS TEST	2
6.1	CONFIGURATION INFORMATION	3
6.2	THE VARIABLE ASSOCIATED DATA TEST	4
6.3	THE VARIABLE PAYLOAD TEST	4
6.4	THE VARIABLE NONCE TEST	5
6.5	THE VARIABLE TAG TEST	6
6.6	THE DECRYPTION-VERIFICATION PROCESS TEST	7
APPENDIX A	REFERENCES	9
APPENDIX B	EXAMPLES OF <i>REQUEST</i>, <i>FAX</i>, <i>RESPONSE</i>, AND <i>SAMPLE FILES</i>	10
B.1	EXAMPLE OF THE <i>REQUEST</i> FILE	10
B.1.1	VADT128.req.....	10
B.1.2	VPT128.req.....	11
B.1.3	VNT128.req.....	13
B.1.4	VTT128.req	14
B.1.5	DVPT128.req.....	16
B.2	EXAMPLE OF THE <i>FAX</i> FILE.....	18
B.2.1	VADT128.fax.....	18
B.2.2	VPT128.fax.....	20
B.2.3	VNT128.fax.....	22
B.2.4	VTT128.req	24
B.2.5	DVPT128.fax.....	26
B.3	EXAMPLE OF THE <i>RESPONSE</i> FILE	29
B.3.1	VADT128.rsp.....	29
B.3.2	VPT128.rsp.....	31
B.3.3	VNT128.rsp.....	33
B.3.4	VTT128.rsp	35
B.3.5	DVPT128.rsp.....	37
B.4	EXAMPLE OF THE <i>SAMPLE</i> FILE	39
B.4.1	VADT128.sam.....	39
B.4.2	VPT128.sam.....	41
B.4.3	VNT128.sam.....	43
B.4.4	VTT128.sam.....	45

B.4.5 DVPT128.sam..... 46

1 Introduction

This document, *The CCM Validation System (CCMVS)* specifies the procedures involved in validating implementations of the CCM Mode of Operation as specified in SP 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality* [1]. The CCMVS is designed to perform automated testing on Implementations Under Test (IUTs). This document provides the basic design and configuration of the CCMVS.

This document defines the purpose, the design philosophy, and the high-level description of the validation process for CCM. The requirements and administrative procedures to be followed by those seeking formal validation of an implementation of CCM are presented. The requirements described include a specification of the data communicated between the IUT and the CCMVS, the details of the tests that the IUT must pass for formal validation, and general instruction for interfacing with the CCMVS. Additionally, an appendix is also provided containing samples of input and output files for the CCMVS.

2 Scope

This document specifies the tests required to validate IUTs for conformance to CCM specified in [1]. When applied to an IUT, the CCMVS provides testing to determine the correctness of the implementation of CCM. The CCMVS is composed of five separate tests – four to test various aspects involved in Encryption-Generation process and one to test the Decryption-Verification process. In addition to performing the tests specified in CCMVS, the IUT must undergo testing of the underlying encryption algorithm, namely AES, implementation via the appropriate validation suite (AESVS).

3 Conformance

The successful completion of the tests contained within the CCMVS and the AESVS is required to be validated as conforming to the CCM standard. Testing for the cryptographic module in which the CCM is implemented is defined in FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*. [2]

4 Definitions and Abbreviations

4.1 Definitions

DEFINITION	MEANING
Advanced Encryption Standard	The algorithm specified in FIPS 197, <i>Advanced Encryption Standard (AES)</i>

CMT laboratory	Cryptographic Module Testing laboratory that operates the CCMVS
----------------	---

4.2 Abbreviations

ABBREVIATION	MEANING
AES	Advanced Encryption Standard specified in FIPS 197
AESVS	Advanced Encryption Standard Validation System
FIPS	Federal Information Processing Standard
CCM	CCM Mode of Operation specified in SP 800-38C
IUT	Implementation Under Test

5 Design Philosophy Of CCM Validation System

The CCMVS is designed to test conformance to the CCM specification rather than provide a measure of a product's security. The validation tests are designed to assist in the detection of accidental implementation errors, and are not designed to detect intentional attempts to misrepresent conformance. Thus, validation should not be interpreted as an evaluation or endorsement of overall product security.

The CCMVS has the following design philosophy:

1. The CCMVS is designed to allow the testing of an IUT at locations remote to the CCMVS. The CCMVS and the IUT communicate data via *REQUEST* and *RESPONSE* files. The CCMVS also generates *SAMPLE* files to provide the IUT with a sample of what the *RESPONSE* file should look like.
2. The testing performed within the CCMVS utilizes statistical sampling (i.e., only a small number of the possible cases are tested); hence, the successful validation of a device does not imply 100% conformance with the standard.

6 CCMVS Test

The CCMVS tests the implementation of CCM for its conformance to the CCM standard. The testing for CCM consists of five tests. These tests are:

- Variable Associated Data Test;
- Variable Payload Test;

- Variable Nonce Test;
- Variable Tag Test; and
- Decryption-Verification Process Test.

6.1 Configuration Information

To initiate the validation process of the CCMVS, a vendor submits an application to an accredited laboratory requesting the validation of its implementation of CCM. The vendor's implementation is referred to as the Implementation Under Test (IUT). The request for validation includes background information describing the IUT along with information needed by the CCMVS to perform the specific tests. More specifically, the request for validation includes:

1. Vendor Name;
2. Product Name;
3. Product Version;
4. Implementation in software, firmware, or hardware;
5. Processor and Operating System with which the IUT was tested if the IUT is implemented in software or firmware;
6. Brief description of the IUT or the product/product family in which the IUT is implemented by the vendor (2-3 sentences); and
7. Configuration information for the CCM tests, including:
 - a) Which AES key sizes are supported: 128, 192, and/or 256;
 - b) Specify a minimum (greater than or equal to zero bytes) and maximum (less than or equal to 32 bytes) associated data length. Additionally, can the implementation handle an associated data length of 2^{16} bytes;
 - c) Specify a minimum (greater than or equal to zero bytes) and maximum (less than or equal to 32 bytes) payload length;
 - d) Specify the nonce lengths supported: 7, 8, 9, 10, 11, 12, and/or 13; and
 - e) Specify the tag lengths supported: 4, 6, 8, 10, 12, 14, and/or 16.

6.2 The Variable Associated Data Test

For each associated data length supported the Variable Associated Data Test provides a 10 sets of associated data and payload to the IUT. The IUT generates a ciphertext as specified by CCM using the data provided. The CCMVS verifies the correctness of the ciphertext produced by the IUT.

The CCMVS:

- A. Creates a *REQUEST* file (Filename: VADT{KeySize}.req) containing:
 - 1. The Product Name;
 - 2. The algorithm being tested; and
 - 3. The keys, nonce, associated data, and payload values to be used as input to the CCM algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

- B. Creates a *FAX* file (Filename: VADT{KeySize}.fax) containing:
 - 1. The information from the *REQUEST* file; and
 - 2. The CT generated by the CCM algorithm.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

- A. Generates the requested CTs using the data specified in the *REQUEST* file.
- B. Creates a *RESPONSE* file (Filename: VADT{KeySize}.rsp) containing:
 - 1. The information from the *REQUEST* file; and
 - 2. The CT generated by the CCM algorithm.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

- A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.
- B. If all values match, records PASS for this test; otherwise, records FAIL.

6.3 The Variable Payload Test

For each payload length supported the Variable Payload Test provides a 10 sets of associated data and payload to the IUT. The IUT generates a ciphertext as specified by CCM using the data provided. The CCMVS verifies the correctness of the ciphertext produced by the IUT.

The CCMVS:

- A. Creates a *REQUEST* file (Filename: VPT{KeySize}.req) containing:
 - 1. The Product Name;
 - 2. The algorithm being tested; and
 - 3. The keys, nonce, associated data, and payload values to be used as input to the CCM algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

- B. Creates a *FAX* file (Filename: VPT{KeySize}.fax) containing:
 - 3. The information from the *REQUEST* file; and
 - 4. The CT generated by the CCM algorithm.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

- A. Generates the requested CTs using the data specified in the *REQUEST* file.
- B. Creates a *RESPONSE* file (Filename: VPT{KeySize}.rsp) containing:
 - 3. The information from the *REQUEST* file; and
 - 4. The CT generated by the CCM algorithm.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

- A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.
- C. B. If all values match, records PASS for this test; otherwise, records FAIL.

6.4 The Variable Nonce Test

For each nonce length supported the Variable Nonce Test provides a 10 sets of associated data and payload to the IUT. The IUT generates a ciphertext as specified by CCM using the data provided. The CCMVS verifies the correctness of the ciphertext produced by the IUT.

The CCMVS:

- A. Creates a *REQUEST* file (Filename: VNT{KeySize}.req) containing:
 - 1. The Product Name;
 - 2. The algorithm being tested; and
 - 3. The keys, nonce, associated data, and payload values to be used as input to the CCM algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

- B. Creates a *FAX* file (Filename: VNT{KeySize}.fax) containing:
 - 5. The information from the *REQUEST* file; and
 - 6. The CT generated by the CCM algorithm.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

- A. Generates the requested CTs using the data specified in the *REQUEST* file.
- B. Creates a *RESPONSE* file (Filename: VNT{KeySize}.rsp) containing:
 - 5. The information from the *REQUEST* file; and
 - 6. The CT generated by the CCM algorithm.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

- A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.
- D. B. If all values match, records PASS for this test; otherwise, records FAIL.

6.5 The Variable Tag Test

For each tag length supported the Variable Tag Test provides a 10 sets of associated data and payload to the IUT. The IUT generates a ciphertext as specified by CCM using the data provided. The CCMVS verifies the correctness of the ciphertext produced by the IUT.

The CCMVS:

- A. Creates a *REQUEST* file (Filename: VTT{KeySize}.req) containing:
 - 1. The Product Name;
 - 2. The algorithm being tested; and
 - 3. The keys, nonce, associated data, and payload values to be used as input to the CCM algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

- B. Creates a *FAX* file (Filename: VTT{KeySize}.fax) containing:
 - 7. The information from the *REQUEST* file; and
 - 8. The CT generated by the CCM algorithm.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

- A. Generates the requested CTs using the data specified in the *REQUEST* file.
- B. Creates a *RESPONSE* file (Filename: VTT{KeySize}.rsp) containing:
 - 7. The information from the *REQUEST* file; and
 - 8. The CT generated by the CCM algorithm.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

- A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.
- E. B. If all values match, records PASS for this test; otherwise, records FAIL.

6.6 The Decryption-Verification Process Test

For each combination of associated data length, payload length, nonce length, and tag length provided as input, 15 sets of input plus ciphertext are supplied to the IUT. The IUT uses the data provided to determine if the ciphertext passes or fails the verification process.

The CCMVS:

- A. Creates a *REQUEST* file (Filename: DVPT{KeySize}.req) containing:
 - 1. The Product Name;
 - 2. The algorithm being tested; and
 - 3. The keys, nonce, associated data, payload, and ciphertext values to be used as input to the decryption-verification process of the CCM algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

- B. Alter some of the ciphertext produced to ensure the decryption-verification process fails
- C. Creates a *FAX* file (Filename: DVPT{KeySize}.fax) containing:
 - 9. The information from the *REQUEST* file; and
 - 10. An indication of whether or not the ciphertext passes to decryption-verification process.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

- A. Performs the decryption-verification process to determine whether the data sets verify correctly or not.

B. Creates a *RESPONSE* file (Filename: DVPT{KeySize}.rsp) containing:

9. The information from the *REQUEST* file; and

10. Whether or not the decryption-verification processed passed or failed.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the CCMVS.

The CCMVS:

A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.

B. If all values match, records PASS for this test; otherwise, records FAIL.

Appendix A References

- [1] *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, Special Publication 800-38C, National Institute of Standards and Technology, May 2004.
- [2] *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2, National Institute of Standards and Technology, May 2001.

Appendix B Examples of *REQUEST*, *FAX*, *RESPONSE*, and *SAMPLE* Files

The following are partial examples of *REQUEST*, *FAX*, *RESPONSE*, and *SAMPLE* files for the HMACVS. Length values are in bytes.

B.1 Example of the *REQUEST* File

B.1.1 VADT128.req

```
# CAVS 4.0
# "CCM-VADT" information for "CCMTest"
# AES Keylen: 128
# Generated on Thu Jul 29 08:03:51 2004

Plen = 32
Nlen = 13
Tlen = 16

[Alen = 0]

Key = 3751c2240d92f4ecdbf5a7824f3d1e6d
Nonce = 92f0935f0e3abc1793e25da5d4

Count = 0
Adata = 00
Payload = 235a8a308fa82bebc614fc79510e7df0456afee923b6a979fdcbc363daa22f8b

Count = 1
Adata = 00
Payload = 47c12148eedaeceb3b90350740ba4f357fe3648a0ae4b7c9e8b92bd6bb8d096e

Count = 2
Adata = 00
Payload = cf54a7b373b8c7b39915853afb4b124cdd9e6f73f00c74b575dd17c3a57deb73

Count = 3
Adata = 00
Payload = 4b5b55d828212b1e3f6310a738f81593c88eb9b386375c36fa24f685f7af086b

Count = 4
Adata = 00
Payload = 259ff0308e071104a5460647b6c7a73f7ab188024653cdf083c53f815ecc9f41

Count = 5
Adata = 00
Payload = 15b201539166a657e29bd6a5a77ed3feec01950b0631cd4ebdc52459b1f2c33e

Count = 6
Adata = 00
Payload = 9552e3087f164bf58bbc3cb3db699ba3209e347518ae593d5576ccc93f48e032
```

```
Count = 7
Adata = 00
Payload = d760547fd96a4b9eb47695b9bb98c3aab09f40c6e5a28f10a2dbd4adc7b89698

Count = 8
Adata = 00
Payload = 502a753b671d3e3d8785e7de14cc84ed705d254fbf59b64dee8c2432f39fc216

Count = 9
Adata = 00
Payload = 3783067c8eab48c2d4c95b82e9d2af7d54b9b865d1e594f209e2ee32a0572221

[Alen = 1]

Key = 01e832095336b761d06f399b279a6d22
Nonce = 20da58d0c347574168b33c4e43

Count = 10
Adata = 95
Payload = aa2253e7e045d7ca29d7166e592f9a856f1e7b146a77d51a5ece7972c67fe3fa

Count = 11
Adata = 1e
Payload = 1446e4da336d243ee01843bc15b116a765c701a37ab00d65c1733bba64e519cb

Count = 12
Adata = 99
Payload = 307dfa454afa61b6475889b5266797254ec73358daf28430347c5b85e59aaec7
.
.
.
```

B.1.2 VPT128.req

```
# CAVS 4.0
# "CCM-VPT" information for "CCMTest"
# AES Keylen: 128
# Generated on Thu Jul 29 08:03:52 2004
```

```
Alen = 32
Nlen = 13
Tlen = 16
```

```
[Plen = 0]
```

```
Key = 2438b445f95ba98fdda32f25e761a5f5
Nonce = 108dce929ea09f3e77be87fe16
```

```
Count = 0
Adata = e1661ae3c88c556bc902cacab56572a5ed9d614ecbb54b3c3de947b9b301d3db
Payload = 00
```

Count = 1
Adata = 938b0cbcc263962a95cfdfe3ee7bf8848199568189cb2621b943e0ca76281f7f
Payload = 00

Count = 2
Adata = 17e20c9ea87ba1ff67d50b936fb0dd3779f42e32fe44e26a9cd52bd8bb814e39
Payload = 00

Count = 3
Adata = e9c6e0ec6bf76e284bdd667ed1f270c40c5a2fe7c50acf30b130ddc6eacf5c75
Payload = 00

Count = 4
Adata = 3ae168d04cae3aea8e79611e35f8c97aaa3f45537fe42586a8610a03e8b9f98d
Payload = 00

Count = 5
Adata = 4435620fdb8a1cb80763f166c85de1cf46615250acf16af064b8ec0a730cd7a
Payload = 00

Count = 6
Adata = 6bfb4fb50e51d2e1ac576096b119e7d9a35442e758d80ebe6730b9dfdc85db53
Payload = 00

Count = 7
Adata = b4044a459bb64273157e8710386ef06d9d0808b4595ea92a2e77ccb203f59f93
Payload = 00

Count = 8
Adata = d65cac0355cecb8768fb4d236f96abbcc9516033eaa09c42aebf3ca7edf6fa85
Payload = 00

Count = 9
Adata = 1aa20368513bbde4177998dae53dfdd99d36efa979049f8b419d3ac1c2f00651
Payload = 00

[Plen = 1]

Key = 8ab59095b6f6c16c37a267b7dc635b80
Nonce = 0b591ac62841e5202c3e155b5c

Count = 10
Adata = ad2d96132445138743b791d154f4cb92073b14a068bcea4e0dfecded947e5292
Payload = 5c

Count = 11
Adata = 4010296f60f3f9d9d0dadcaa3270210000dbab44ccec52ffcc9986ef95ae355b
Payload = 33

Count = 12
Adata = 80fb10b3da25359e47920cfcfbf15a5149bb8731b493f34b88f18da73cbfa12c
Payload = 83

.
.

B.1.3 VNT128.req

```
# CAVS 4.0
# "CCM-VNT" information for "CCMTest"
# AES Keylen: 128
# Generated on Thu Jul 29 08:03:52 2004
```

```
Alen = 32
Plen = 32
Tlen = 16
```

```
[Nlen = 7]
```

```
Key = f53c712b9f4b5c5e6cf27ef3f8ac73ea
```

```
Count = 0
Nonce = db3e34e6404c8e
Adata = 0c7316150d38b0cf8df11c0a9dbb1078bc6b20274a2cd84b3f6a083e1cef5fc5
Payload = 0250670e86463e9dd98807d8a8e0f085aeebb8b2cdd5679f5d643dd8c438e8a2
```

```
Count = 1
Nonce = ad8f2a8810023d
Adata = c3ec92aced686e68067a663aa1b7c8099ad77de64f18e0910dddd13fc99b049a
Payload = 38fda30748eabf412fba06874ae06c0dcc5752c2be92a9dd45b55bb82405e6e2
```

```
Count = 2
Nonce = 0915baald7245e
Adata = b2207f9c0f0426f171ff18b2a4392f61fb4ee4a44c476fe03dc93009be8c4eb9
Payload = 6a2f9201da0fa4f8b1962a58feaa41576f4db529b9717c733a0e8302dd73aebd
```

```
Count = 3
Nonce = e9b76ca0f93cfb
Adata = 6c05dd99097ccb16fda6819ac39d022920a4d344635d5fbbec3c9ac3eb3be548
Payload = 965b71f155ee858955d652d693efd13cf35c27a0d4ced5cee6022f18408c0f40
```

```
Count = 4
Nonce = f552bf199d0ac6
Adata = b0eb93c330a111a4b2e527fd19a06a1c46bc6964dedc8fa34e4a4b9f0d306df2
Payload = bfd1e7f5478b010a20f719f11f284186790b0630cd54987265b82bbdb95d9c89
```

```
Count = 5
Nonce = 46dc5c84c5c3b1
Adata = e9d74e527a15ff43e276570b5ad70e91046cdcc2e4b396282ba69bbfbc356e05
Payload = e85bb8b3fc20aa5cc0dbaa0aeeebec30fd7d3981a200930598d91c6d9d5834a4
```

```
Count = 6
Nonce = ec84e37cfe420c
Adata = 42a4c249ff283c068c7d8e5ed5eab2f64149e5a79560ab73156f13beec063cba
Payload = 12a3d7b4227c6fbecf5196969a3368fd11068719963405c462a3842acae49b93
```

```
Count = 7
```

Nonce = 20809dfd638e24
Adata = 4f5331899a4cf958fb0099819ef94302da469b8011cdbc39d8e37b3a581aefd2
Payload = 150133285890c10c4541886d3f3c1e5ca2bbe287fa6ed8b8731fb49e919234d0

Count = 8
Nonce = 17c329e64cf55c
Adata = 5752565d411ca6a6fd67860041e57540a1a4d391a9d8985f29db4574d0721b61
Payload = 0ea808ce758a65f491ca2185d171385c35cdcce6035c762abcecd064eff7ebb

Count = 9
Nonce = 77279387f30a1f
Adata = f38ce2ed5868711988f2c49209eaa8be378e756b36be9c122b5e805dacfc87e6
Payload = 4ad33e1b998b6014d0c4614db0c5bc67245f4ae28123aeea0cd2f074bd15688a

[Nlen = 8]

Key = f0bc7ebd9f8ac31a42b646be0a78eb4f

Count = 10
Nonce = 1b587128ad11400e
Adata = 3029db22aba5ebab2053f39b7b07c97de7cba2c5d9d3326451af149a5dc46b0b
Payload = 7d3098cb1fc5a1954aea7d5b2ede03e38839fa2a75728b0288a4f5ff1a928394

Count = 11
Nonce = c3be3ba92028b748
Adata = f2448f99a631ee4a6c95e154ea8de0dcfc97446c56a407a46b6fcc2d8e0c1fef
Payload = 859157f53a401a7a8706044aa24e9e64e2259743240351556de8a0afd1abceff

Count = 12
Nonce = 093983c684e75dcb
Adata = 550cfc1e529b013fa8b5a5bd2c67122df500ab771cc5f029c0e6a2114db1280a
Payload = 580bbe3260a80738ee5b12e6b2e727b8464bdb40064484c82213f039f280573b

.
. .

B.1.4 VTT128.req

```
# CAVS 4.0  
# "CCM-VTT" information for "CCMTest"  
# AES Keylen: 128  
# Generated on Thu Jul 29 08:03:52 2004
```

Alen = 32
Plen = 32
Nlen = 13

[Tlen = 4]

Key = 0ca55a6d8e5104a586c5d00b364fa187
Nonce = 8b2f2d20703538ea929312bb3e

Count = 0

Adata = 89182405c706aacab3cbf8425fc745dd4ffdd3e07d0c17ffa0621a2daeac1fb3
Payload = b6fa778f4bfc6dfe4d4aca505d4b6bbf57c413d23cf903977015cb2d26cb5f86

Count = 1

Adata = fadf339fd4bd94c5c1147a97026e5399981c3d3fb4d71cb36fa7e9d2bb044d77
Payload = 23f8fb9b2cdaa10715e08b94d0c5dbea3b7ffbdea2ba3b8d8584bca79c4a8e0e

Count = 2

Adata = e66a77b24b5899c8d2a356fd36acd7df9d940fac1aac5668762d532c302a20c1
Payload = 536fd560b83ac5dd9bc3d205786a66e73741e1b648cc46b8f205345ee8a319b5

Count = 3

Adata = d23093e1c5258caf72151a2dbe206b245a03d9d5989a62977ea358c11ac459ca
Payload = e6184bc8c178alaba852a239941027b15788b84dd2695dc669d9b21bb45c3a8f

Count = 4

Adata = 49fafa6fa7685b8ebd09090fe0f396c5e4b623e28431dd6a03abc8e7141fbc5f
Payload = a5df31a9a76e0ad25429c900ca0f87b901812d1545eb877deaa69ab33b1d3812

Count = 5

Adata = 333711870519a55637e750537f8f1803a1d8758490f4a0c3d6580def37cb362d
Payload = ce7877b9a86a67d6c3fb4aaa17d86b5fedb3035ce6385dd14043388f55506d1e

Count = 6

Adata = 0e2885db43bb745831059c13aae17969282e82c0052c010fee2923a2955e4b17
Payload = c21454e083330abb387f22c2790306051fff87659debceb194b8950fa159979e

Count = 7

Adata = ed4db3dd7fab9e52bc636e3b37887bdb3d039c0369d9537a73ac44a14985ec57
Payload = bde29a2eab396e652f74a73a70ad49b03a12178ffdddb400198608575836e530

Count = 8

Adata = 80f8235f264c99e80968348b040ebdbe430be04bf71682544efc5495a2faa8ea
Payload = de182cda7c44d5966476be9f4043755baa69158937bd6ad5b46555a9af477247

Count = 9

Adata = d8cb7cb847410e6a3f78502d9ea0483ec07b362c07acca3bbb3295061530be69
Payload = 8f45f26fa0822c2a73428697fa7e9c30da17626cc2d315e0fba271aa4127250f

[Tlen = 6]

Key = 3619dd376a7902385531b5d0b9c6f458

Nonce = 200e953c0616887f2832f24be7

Count = 10

Adata = 270338ecc3987e4a64cbe751c96ec4a06539c5b905d5bcb3b433a530db22e48f
Payload = 987d0205bdffea464c978e4f8ffa2491fe4e898304df27f506131ca2a2a09904

Count = 11

Adata = 21b788ca8e96b71d3ecd78de27ca96837a4be65dd6c41d19bb00e48d410a2fb2
Payload = ddaff7d549344f595c5df062bffd2f8650df7881df45e426306b9bf7c4a81e7

Count = 12

Adata = 9dabcf6f967c6ca60c0e1ca329b27be58968171049a625d76154731e341b9e60

Payload = 903b2599d8b7f78eefcedd9cc8797b2259a49e09f1332deecc435d83e5b22332
.
.
.

B.1.5 DVPT128.req

```
# CAVS 4.0
# "CCM-DVPT" information for "CCMTest"
# AES Keylen: 128
# Generated on Thu Jul 29 08:03:52 2004
```

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 4]

Key = 0cb1e2654c33da429ebef20b53b121a8

```
Count = 0
Nonce = afe6f12d0ea174
Adata = 00
Payload = 00
CT = ab72b36b
```

```
Count = 1
Nonce = da7dfe30a59977
Adata = 00
Payload = 00
CT = 5de8d3e2
```

```
Count = 2
Nonce = 753ded3501a6ca
Adata = 00
Payload = 00
CT = a44784a4
```

```
Count = 3
Nonce = 49a7e02c8f0186
Adata = 00
Payload = 00
CT = 0d1331c9
```

```
Count = 4
Nonce = 688a92a78e57b2
Adata = 00
Payload = 00
CT = dd507b85
```

```
Count = 5
Nonce = 8c84018b595ff1
Adata = 00
Payload = 00
CT = b49eb878
```

Count = 6
Nonce = f06f3e1b1428e5
Adata = 00
Payload = 00
CT = c5d14a98

Count = 7
Nonce = b5430fb552c2cc
Adata = 00
Payload = 00
CT = 7419968c

Count = 8
Nonce = 87e3324b5fb4f5
Adata = 00
Payload = 00
CT = c40e6e92

Count = 9
Nonce = a3ac390add8073
Adata = 00
Payload = 00
CT = 84fe8dd3

Count = 10
Nonce = ae69674ea08a60
Adata = 00
Payload = 00
CT = 4e021854

Count = 11
Nonce = ae4d72eaf8dcb7
Adata = 00
Payload = 00
CT = acc80bca

Count = 12
Nonce = 9c42a04aeb5b86
Adata = 00
Payload = 00
CT = c6458ec7

Count = 13
Nonce = 594b76db2d290e
Adata = 00
Payload = 00
CT = 2ed90865

Count = 14
Nonce = 709e122f1d714c
Adata = 00
Payload = 00
CT = c0610700

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 16]

Key = 50de369adcba6018a7c9214de0cf3ac1

Count = 15

Nonce = afe6f12d0ea174

Adata = 00

Payload = 00

CT = 1610970994a785163d128b22cf21d535

Count = 16

Nonce = da7dfe30a59977

Adata = 00

Payload = 00

CT = 941bd3b74ceaf849d39bdd29b8fb0869

Count = 17

Nonce = 753ded3501a6ca

Adata = 00

Payload = 00

CT = dc2c46d367f346977602bff216097b47

.
. .
.

B.2 Example of the FAX File

B.2.1 VADT128.fax

```
# CAVS 4.0
# "CCM-VADT" information for "CCMTest"
# AES Keylen: 128
# Generated on Thu Jul 29 08:03:51 2004
```

Plen = 32

Nlen = 13

Tlen = 16

[Alen = 0]

Key = 3751c2240d92f4ecdbf5a7824f3d1e6d

Nonce = 92f0935f0e3abc1793e25da5d4

Count = 0

Adata = 00

Payload = 235a8a308fa82bebc614fc79510e7df0456afee923b6a979fdcbc363daa22f8b

CT =

b0e5e3f8d507678a8ec90d26ebe8f6855cc4e4da5a6f81bdf4fa374e34ba728ad513502c1b5c57
33297d9f7e66907202

Count = 1

Adata = 00

Payload = 47c12148eedaeceb3b90350740ba4f357fe3648a0ae4b7c9e8b92bd6bb8d096e

CT =
d47e4880b475a08a734dc458fa5cc440664d7eb9733d9f0de188dfffb5595546f3f99884861eb40
4ee4410fd7dd999ad5

Count = 2
Adata = 00
Payload = cf54a7b373b8c7b39915853afb4b124cdd9e6f73f00c74b575dd17c3a57deb73
CT =
5cebce7b29178bd2d1c8746541ad9939c430754089d55c717cece3ee4b65b672747b4d9822dd88
6f799ce23a2c5a4065

Count = 3
Adata = 00
Payload = 4b5b55d828212b1e3f6310a738f81593c88eb9b386375c36fa24f685f7af086b
CT =
d8e43c10728e677f77bee1f8821e9ee6d120a380ffee74f2f31502a819b7556adcbb4857292162
077be8abfaa51e9ef6

Count = 4
Adata = 00
Payload = 259ff0308e071104a5460647b6c7a73f7ab188024653cdf083c53f815ecc9f41
CT =
b62099f8d4a85d65ed9bf7180c212c4a631f92313f8ae5348af4cbacb0d4c2402b4039966a39bd
ec0187b76cbfec6a0

Count = 5
Adata = 00
Payload = 15b201539166a657e29bd6a5a77ed3feec01950b0631cd4ebdc52459b1f2c33e
CT =
860d689bcb9ea36aa4627fa1d98588bf5af8f387fe8e58ab4f4d0745fea9e3f95b698e9c2b080
c2694db82dcd58aaf1

Count = 6
Adata = 00
Payload = 9552e3087f164bf58bbc3cb3db699ba3209e347518ae593d5576ccc93f48e032
CT =
06ed8ac025b90794c361cdec618f10d639302e46617771f95c4738e4d150bd33a6929e342dd2e9
0012ce931a1a4a64ad

Count = 7
Adata = 00
Payload = d760547fd96a4b9eb47695b9bb98c3aab09f40c6e5a28f10a2dbd4adc7b89698
CT =
44df3db783c507fffcab64e6017e48dfa9315af59c7ba7d4abea208029a0cb99ef9c7f779398f3
9fb223562e7811649d

Count = 8
Adata = 00
Payload = 502a753b671d3e3d8785e7de14cc84ed705d254fbf59b64dee8c2432f39fc216
CT =
c3951cf33db2725ccf581681ae2a0f9869f33f7cc6809e89e7bdd01f1d879f171bf2a11ca9b4d7
80c2c93a91428a459a

Count = 9

Adata = 00
Payload = 3783067c8eab48c2d4c95b82e9d2af7d54b9b865d1e594f209e2ee32a0572221
CT =
a43c6fb4d40404a39c14aadd533424084d17a256a83cbc3600d31a1f4e4f7f205be0b4de08344a
6716a639465df352d0

[Alen = 1]

Key = 01e832095336b761d06f399b279a6d22
Nonce = 20da58d0c347574168b33c4e43

Count = 10
Adata = 95
Payload = aa2253e7e045d7ca29d7166e592f9a856f1e7b146a77d51a5ece7972c67fe3fa
CT =
f7658c566c0823b7f41a5e4cddf4d4a5e749546b3f6d2eccf6481065c2597ba2caa5a2c7843d1f
c09569a27ce465cfb9

Count = 11
Adata = 1e
Payload = 1446e4da336d243ee01843bc15b116a765c701a37ab00d65c1733bba64e519cb
CT =
49013b6bbf20d0433dd50b9e916a5887ed902edc2faaf6b369f552ad60c38193a163875d91e365
2b5bb3dcad97e93b61

Count = 12
Adata = 99
Payload = 307dfa454afa61b6475889b5266797254ec73358daf28430347c5b85e59aaec7
CT =
6d3a25f4c6b795cb9a95c197a2bcd905c6901c278fe87fe69cfa3292e1bc369f7975cb299dc8ef
5419e488623d86388b

.
. .
.

B.2.2 VPT128.fax

CAVS 4.0
"CCM-VPT" information for "CCMTest"
AES Keylen: 128
Generated on Thu Jul 29 08:03:52 2004

Alen = 32
Nlen = 13
Tlen = 16

[Plen = 0]

Key = 2438b445f95ba98fdda32f25e761a5f5
Nonce = 108dce929ea09f3e77be87fe16

Count = 0
Adata = e1661ae3c88c556bc902cacab56572a5ed9d614ecbb54b3c3de947b9b301d3db

Payload = 00
CT = 9ef776fe20a953e153461f68685fd56f

Count = 1
Adata = 938b0cbcc263962a95cfdfe3ee7bf8848199568189cb2621b943e0ca76281f7f
Payload = 00
CT = 2786f31a04dfac83750cdd4dee02de8d

Count = 2
Adata = 17e20c9ea87ba1ff67d50b936fb0dd3779f42e32fe44e26a9cd52bd8bb814e39
Payload = 00
CT = d808677b9a960feac77a4afcc4901163

Count = 3
Adata = e9c6e0ec6bf76e284bdd667ed1f270c40c5a2fe7c50acf30b130ddc6eacf5c75
Payload = 00
CT = b5deaf1c2c2660448d62315614bc9c40

Count = 4
Adata = 3ae168d04cae3aea8e79611e35f8c97aaa3f45537fe42586a8610a03e8b9f98d
Payload = 00
CT = 2b337f5a6f4d22b08869b2ed453b144b

Count = 5
Adata = 4435620fdb8a1cb80763f166c85de1cf46615250acf16af064b8ec0a730cd7a
Payload = 00
CT = d9d047a6943a21c107119304f9538f01

Count = 6
Adata = 6bfb4fb50e51d2e1ac576096b119e7d9a35442e758d80ebe6730b9dfdc85db53
Payload = 00
CT = 1c70d0329b21ae05c1664a233dade23b

Count = 7
Adata = b4044a459bb64273157e8710386ef06d9d0808b4595ea92a2e77ccb203f59f93
Payload = 00
CT = a8e5ac484fd2ce45d6e9a15dbdbf8283

Count = 8
Adata = d65cac0355cecb8768fb4d236f96abbcc9516033eaa09c42aebf3ca7edf6fa85
Payload = 00
CT = 9f02e81c4c1e85623e94ab69734eb2e3

Count = 9
Adata = 1aa20368513bbde4177998dae53dfdd99d36efa979049f8b419d3ac1c2f00651
Payload = 00
CT = ebcc27d11c4a094e54339f974430dd21

[Plen = 1]

Key = 8ab59095b6f6c16c37a267b7dc635b80
Nonce = 0b591ac62841e5202c3e155b5c

Count = 10

Adata = ad2d96132445138743b791d154f4cb92073b14a068bcea4e0dfecded947e5292
Payload = 5c
CT = 331424d3e5f3d0dcd8bb954985e2a701e7

Count = 11
Adata = 4010296f60f3f9d9d0dadcaa3270210000dbab44ccec52ffcc9986ef95ae355b
Payload = 33
CT = 5ca30976a7e77d01e8a851a27e4abef31a

Count = 12
Adata = 80fb10b3da25359e47920cfcfbf15a5149bb8731b493f34b88f18da73cbfa12c
Payload = 83
CT = ecc0d9b5e2f2ac20b700c18a0c36d16e95

.
.
.

B.2.3 VNT128.fax

CAVS 4.0
"CCM-VNT" information for "CCMTest"
AES Keylen: 128
Generated on Thu Jul 29 08:03:52 2004

Alen = 32
Plen = 32
Tlen = 16

[Nlen = 7]

Key = f53c712b9f4b5c5e6cf27ef3f8ac73ea

Count = 0
Nonce = db3e34e6404c8e
Adata = 0c7316150d38b0cf8df11c0a9dbb1078bc6b20274a2cd84b3f6a083e1cef5fc5
Payload = 0250670e86463e9dd98807d8a8e0f085aeebb8b2cdd5679f5d643dd8c438e8a2
CT =
c300313252c9073c1d6a51478ac6221d3c1292d07a5c8c6c4b57a81eea62cb7d230c0a1aa08681
a328f8708a0fa6d074

Count = 1
Nonce = ad8f2a8810023d
Adata = c3ec92aced686e68067a663aa1b7c8099ad77de64f18e0910dddd13fc99b049a
Payload = 38fda30748eabf412fba06874ae06c0dcc5752c2be92a9dd45b55bb82405e6e2
CT =
6fd70b2f43b7372c1da42788709c665e165995238693aaae29e44e8120c07dc93385afe91f8363
d1e3751195d6fd49a8

Count = 2
Nonce = 0915baald7245e
Adata = b2207f9c0f0426f171fff18b2a4392f61fb4ee4a44c476fe03dc93009be8c4eb9
Payload = 6a2f9201da0fa4f8b1962a58feaa41576f4db529b9717c733a0e8302dd73aebd

CT =
116ecedb4236068cf0f58e775770710be775d5d9091ee457df067204d053aa9e1fbb531662b3fa
a5e4f9083d704f3b69

Count = 3
Nonce = e9b76ca0f93cfb
Adata = 6c05dd99097ccb16fda6819ac39d022920a4d344635d5fbbec3c9ac3eb3be548
Payload = 965b71f155ee858955d652d693efd13cf35c27a0d4ced5cee6022f18408c0f40
CT =
e081a95a986691fa9c0dc95051a7350814e78813c18140765f2c0c6154927e900352f6ea139192
3a243746c57026f835

Count = 4
Nonce = f552bf199d0ac6
Adata = b0eb93c330a111a4b2e527fd19a06a1c46bc6964dedc8fa34e4a4b9f0d306df2
Payload = bfd1e7f5478b010a20f719f11f284186790b0630cd54987265b82bbdb95d9c89
CT =
00b1b5ea9ae7b9ebbf55f4742f9fe0c5789a3ddf821eaba2c1c1b018169241cd07d5d8bb588129
d7439ccda3596e4bd1

Count = 5
Nonce = 46dc5c84c5c3b1
Adata = e9d74e527a15ff43e276570b5ad70e91046cdcc2e4b396282ba69bbfbc356e05
Payload = e85bb8b3fc20aa5cc0dbaa0aeecbec30fd7d3981a200930598d91c6d9d5834a4
CT =
c6af9e02df383b29a6f634b0c501e1e92c1001282c557b1d8150e8e104d2e906059602aff5bd28
efb401ae8222e91780

Count = 6
Nonce = ec84e37cfe420c
Adata = 42a4c249ff283c068c7d8e5ed5eab2f64149e5a79560ab73156f13beec063cba
Payload = 12a3d7b4227c6fbecf5196969a3368fd11068719963405c462a3842acae49b93
CT =
287a20ddee78a2e898b80244540a68ab48f994ea7df5fa7e584fd6d4572cdc70c0e72ad230bce6
15eb36bf7895a5db68

Count = 7
Nonce = 20809dfd638e24
Adata = 4f5331899a4cf958fb0099819ef94302da469b8011cdbc39d8e37b3a581aefd2
Payload = 150133285890c10c4541886d3f3c1e5ca2bbe287fa6ed8b8731fb49e919234d0
CT =
b3f483e32a60f8e78311d860f017509c60d128c317952171697e19115afb311caa6d64d375621c
a58957e1f546086a20

Count = 8
Nonce = 17c329e64cf55c
Adata = 5752565d411ca6a6fd67860041e57540a1a4d391a9d8985f29db4574d0721b61
Payload = 0ea808ce758a65f491ca2185d171385c35cdcce6035c762abcecdca064eff7ebb
CT =
0dd33d4a13e2952c838d1aeaf3c4301339408e059b83820622d125823cd93e7de42adff61fd84e
1ebbef01daa1b7df85

Count = 9
Nonce = 77279387f30a1f

```
Adata = f38ce2ed5868711988f2c49209eaa8be378e756b36be9c122b5e805dacfc87e6
Payload = 4ad33e1b998b6014d0c4614db0c5bc67245f4ae28123aeea0cd2f074bd15688a
CT =
a2e54c80610d9d3e2dc92eb6ab3d0633bad5cde39df576c1ae1d9a48de01fc37667c6046d9ae47
6010e1891d5b3c27d3
```

```
[Nlen = 8]
```

```
Key = f0bc7ebd9f8ac31a42b646be0a78eb4f
```

```
Count = 10
```

```
Nonce = 1b587128ad11400e
```

```
Adata = 3029db22aba5ebab2053f39b7b07c97de7cba2c5d9d3326451af149a5dc46b0b
```

```
Payload = 7d3098cb1fc5a1954aea7d5b2ede03e38839fa2a75728b0288a4f5ff1a928394
```

```
CT =
```

```
2221c311f7bba4eed9aa83caceafcf6e4e5f641f20ae2217232c0e51f851d19549bb1b4e0f122
affe20e2324fe0e7fd
```

```
Count = 11
```

```
Nonce = c3be3ba92028b748
```

```
Adata = f2448f99a631ee4a6c95e154ea8de0dcfc97446c56a407a46b6fcc2d8e0c1fef
```

```
Payload = 859157f53a401a7a8706044aa24e9e64e2259743240351556de8a0afd1abceff
```

```
CT =
```

```
e23efbc1040d85d2d2227626e44ebcc296f372d1b5bb89a904789c51f4abf72ca5cc836041abd8
99b64f8b7db9323aa8
```

```
Count = 12
```

```
Nonce = 093983c684e75dcb
```

```
Adata = 550cfc1e529b013fa8b5a5bd2c67122df500ab771cc5f029c0e6a2114db1280a
```

```
Payload = 580bbe3260a80738ee5b12e6b2e727b8464bdb40064484c82213f039f280573b
```

```
CT =
```

```
27e04d474cd9d46b854851656c0925ce9d91e825d636254e4d81bc2210818017852c2be0f32775
2f0b784fb205898afd
```

```
.
.
.
```

B.2.4 VTT128.req

```
# CAVS 4.0
```

```
# "CCM-VTT" information for "CCMTest"
```

```
# AES Keylen: 128
```

```
# Generated on Thu Jul 29 08:03:52 2004
```

```
Alen = 32
```

```
Plen = 32
```

```
Nlen = 13
```

```
[Tlen = 4]
```

```
Key = 0ca55a6d8e5104a586c5d00b364fa187
```

```
Nonce = 8b2f2d20703538ea929312bb3e
```

Count = 0
Adata = 89182405c706aacab3cbf8425fc745dd4ffdd3e07d0c17ffa0621a2daeac1fb3
Payload = b6fa778f4bfc6dfe4d4aca505d4b6bbf57c413d23cf903977015cb2d26cb5f86
CT = 5faa490e44a1e88989b329ae87f215255b46450642fc779eac2d8b0220a65b84f011348a

Count = 1
Adata = fadf339fd4bd94c5c1147a97026e5399981c3d3fb4d71cb36fa7e9d2bb044d77
Payload = 23f8fb9b2cdaa10715e08b94d0c5dbea3b7ffbdea2ba3b8d8584bca79c4a8e0e
CT = caa8c51a23872470d119686a0a7ca57037fdad0adcbf4f8459bcfc889a278a0c7962dcbd

Count = 2
Adata = e66a77b24b5899c8d2a356fd36acd7df9d940fac1aac5668762d532c302a20c1
Payload = 536fd560b83ac5dd9bc3d205786a66e73741e1b648cc46b8f205345ee8a319b5
CT = ba3febelb76740aa5f3a31fba2d3187d3bc3b76236c932b12e3d7471eece1db775651fe4

Count = 3
Adata = d23093e1c5258caf72151a2dbe206b245a03d9d5989a62977ea358c11ac459ca
Payload = e6184bc8c178alaba852a239941027b15788b84dd2695dc669d9b21bb45c3a8f
CT = 0f487549ce2524dc6cab41c74ea9592b5b0aee99ac6c29cfb5e1f234b2313e8d81911408

Count = 4
Adata = 49fafa6fa7685b8ebd09090fe0f396c5e4b623e28431dd6a03abc8e7141fbc5f
Payload = a5df31a9a76e0ad25429c900ca0f87b901812d1545eb877deaa69ab33b1d3812
CT = 4c8f0f28a8338fa590d02afe10b6f9230d037bc13beef374369eda9c3d703c10ee97a2a5

Count = 5
Adata = 333711870519a55637e750537f8f1803a1d8758490f4a0c3d6580def37cb362d
Payload = ce7877b9a86a67d6c3fb4aaa17d86b5fedb3035ce6385dd14043388f55506d1e
CT = 27284938a737e2a10702a954cd6115c5e1315588983d29d89c7b78a0533d691c6db2f4ca

Count = 6
Adata = 0e2885db43bb745831059c13aae17969282e82c0052c010fee2923a2955e4b17
Payload = c21454e083330abb387f22c2790306051fff87659debceb194b8950fa159979e
CT = 2b446a618c6e8fccfc86c13ca3ba789f137dd1b1e3eebab84880d520a734939c23015a32

Count = 7
Adata = ed4db3dd7fab9e52bc636e3b37887bdb3d039c0369d9537a73ac44a14985ec57
Payload = bde29a2eab396e652f74a73a70ad49b03a12178ffdddb400198608575836e530
CT = 54b2a4afa464eb12eb8d44c4aa14372a3690415b83d8c009c5be48785e5be1321ad451e8

Count = 8
Adata = 80f8235f264c99e80968348b040ebdbe430be04bf71682544efc5495a2faa8ea
Payload = de182cda7c44d5966476be9f4043755baa69158937bd6ad5b46555a9af477247
CT = 3748125b731950e1a08f5d619afa0bc1a6eb435d49b81edc685d1586a92a764501cab1d1

Count = 9
Adata = d8cb7cb847410e6a3f78502d9ea0483ec07b362c07acca3bbb3295061530be69
Payload = 8f45f26fa0822c2a73428697fa7e9c30da17626cc2d315e0fba271aa4127250f
CT = 6615cceeafdfa95db7bb656920c7e2aad69534b8bcd661e9279a3185474a210d329b27f6

[Tlen = 6]

Key = 3619dd376a7902385531b5d0b9c6f458
Nonce = 200e953c0616887f2832f24be7

Count = 10
Adata = 270338ecc3987e4a64cbe751c96ec4a06539c5b905d5bcb3b433a530db22e48f
Payload = 987d0205bdffea464c978e4f8ffa2491fe4e898304df27f506131ca2a2a09904
CT =
5f3c0e7c4cf305756c93783cbfe31f0c6fa56a325c37bf2b7b9571c51caa7124351942e7d253

Count = 11
Adata = 21b788ca8e96b71d3ecd78de27ca96837a4be65dd6c41d19bb00e48d410a2fb2
Payload = ddaff7d549344f595c5df062bffd2f8650df7881df45e426306b9bf7c4a81e7
CT =
1aeefbacb838a06a7c5906118fe4c965f4e61439451cc69c1e80d4d8c24069c76b57cc5b2541

Count = 12
Adata = 9dabcf6f967c6ca60c0e1ca329b27be58968171049a625d76154731e341b9e60
Payload = 903b2599d8b7f78eefcedd9cc8797b2259a49e09f1332deecc435d83e5b22332
CT =
577a29e029bb18bdcfca2beff86040bfc84f7db8a9dbb530b1c530e45bb8cb12f3eb94386919

.
. .

B.2.5 DVPT128.fax

```
# CAVS 4.0  
# "CCM-DVPT" information for "CCMTest"  
# AES Keylen: 128  
# Generated on Thu Jul 29 08:03:52 2004
```

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 4]

Key = 0cb1e2654c33da429ebef20b53b121a8

Count = 0
Nonce = afe6f12d0ea174
Adata = 00
Payload = 00
CT = ab72b36b
Result = Pass

Count = 1
Nonce = da7dfe30a59977
Adata = 00
Payload = 00
CT = 5de8d3e2
Result = Fail

Count = 2
Nonce = 753ded3501a6ca
Adata = 00
Payload = 00

CT = a44784a4
Result = Pass

Count = 3
Nonce = 49a7e02c8f0186
Adata = 00
Payload = 00
CT = 0d1331c9
Result = Fail

Count = 4
Nonce = 688a92a78e57b2
Adata = 00
Payload = 00
CT = dd507b85
Result = Pass

Count = 5
Nonce = 8c84018b595ff1
Adata = 00
Payload = 00
CT = b49eb878
Result = Fail

Count = 6
Nonce = f06f3e1b1428e5
Adata = 00
Payload = 00
CT = c5d14a98
Result = Fail

Count = 7
Nonce = b5430fb552c2cc
Adata = 00
Payload = 00
CT = 7419968c
Result = Fail

Count = 8
Nonce = 87e3324b5fb4f5
Adata = 00
Payload = 00
CT = c40e6e92
Result = Fail

Count = 9
Nonce = a3ac390add8073
Adata = 00
Payload = 00
CT = 84fe8dd3
Result = Pass

Count = 10
Nonce = ae69674ea08a60

Adata = 00
Payload = 00
CT = 4e021854
Result = Pass

Count = 11
Nonce = ae4d72eaf8dcb7
Adata = 00
Payload = 00
CT = acc80bca
Result = Fail

Count = 12
Nonce = 9c42a04aeb5b86
Adata = 00
Payload = 00
CT = c6458ec7
Result = Fail

Count = 13
Nonce = 594b76db2d290e
Adata = 00
Payload = 00
CT = 2ed90865
Result = Fail

Count = 14
Nonce = 709e122f1d714c
Adata = 00
Payload = 00
CT = c0610700
Result = Fail

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 16]

Key = 50de369adcba6018a7c9214de0cf3ac1

Count = 15
Nonce = afe6f12d0ea174
Adata = 00
Payload = 00
CT = 1610970994a785163d128b22cf21d535
Result = Pass

Count = 16
Nonce = da7dfe30a59977
Adata = 00
Payload = 00
CT = 941bd3b74ceaf849d39bdd29b8fb0869
Result = Fail

Count = 17
Nonce = 753ded3501a6ca
Adata = 00

```
Payload = 00
CT = dc2c46d367f346977602bff216097b47
Result = Pass
.
.
.
```

B.3 Example of the *RESPONSE* File

B.3.1 VADT128.rsp

```
# CAVS 4.0
# "CCM-VADT" information for "CCMTest"
# AES Keylen: 128

Plen = 32
Nlen = 13
Tlen = 16

[Alen = 0]

Key = 3751c2240d92f4ecdbf5a7824f3d1e6d
Nonce = 92f0935f0e3abc1793e25da5d4

Count = 0
Adata = 00
Payload = 235a8a308fa82bebc614fc79510e7df0456afee923b6a979fdcbc363daa22f8b
CT =
b0e5e3f8d507678a8ec90d26ebe8f6855cc4e4da5a6f81bdf4fa374e34ba728ad513502c1b5c57
33297d9f7e66907202

Count = 1
Adata = 00
Payload = 47c12148eedaeceb3b90350740ba4f357fe3648a0ae4b7c9e8b92bd6bb8d096e
CT =
d47e4880b475a08a734dc458fa5cc440664d7eb9733d9f0de188dfffb5595546f3f99884861eb40
4ee4410fd7dd999ad5

Count = 2
Adata = 00
Payload = cf54a7b373b8c7b39915853afb4b124cdd9e6f73f00c74b575dd17c3a57deb73
CT =
5cebce7b29178bd2d1c8746541ad9939c430754089d55c717cece3ee4b65b672747b4d9822dd88
6f799ce23a2c5a4065

Count = 3
Adata = 00
Payload = 4b5b55d828212b1e3f6310a738f81593c88eb9b386375c36fa24f685f7af086b
CT =
d8e43c10728e677f77bee1f8821e9ee6d120a380ffee74f2f31502a819b7556adcbb4857292162
077be8abfaa51e9ef6

Count = 4
```

Adata = 00
Payload = 259ff0308e071104a5460647b6c7a73f7ab188024653cdf083c53f815ecc9f41
CT =
b62099f8d4a85d65ed9bf7180c212c4a631f92313f8ae5348af4cbacb0d4c2402b4039966a39bd
ec0187b76cbfeca6a0

Count = 5
Adata = 00
Payload = 15b201539166a657e29bd6a5a77ed3feec01950b0631cd4ebdc52459b1f2c33e
CT =
860d689bc9ea36aa4627fa1d98588bf5af8f387fe8e58ab4f4d0745fea9e3f95b698e9c2b080
c2694db82dcd58aaf1

Count = 6
Adata = 00
Payload = 9552e3087f164bf58bbc3cb3db699ba3209e347518ae593d5576ccc93f48e032
CT =
06ed8ac025b90794c361cdec618f10d639302e46617771f95c4738e4d150bd33a6929e342dd2e9
0012ce931a1a4a64ad

Count = 7
Adata = 00
Payload = d760547fd96a4b9eb47695b9bb98c3aab09f40c6e5a28f10a2dbd4adc7b89698
CT =
44df3db783c507fffcab64e6017e48dfa9315af59c7ba7d4abea208029a0cb99ef9c7f779398f3
9fb223562e7811649d

Count = 8
Adata = 00
Payload = 502a753b671d3e3d8785e7de14cc84ed705d254fbf59b64dee8c2432f39fc216
CT =
c3951cf33db2725ccf581681ae2a0f9869f33f7cc6809e89e7bdd01f1d879f171bf2a11ca9b4d7
80c2c93a91428a459a

Count = 9
Adata = 00
Payload = 3783067c8eab48c2d4c95b82e9d2af7d54b9b865d1e594f209e2ee32a0572221
CT =
a43c6fb4d40404a39c14aadd533424084d17a256a83cbc3600d31a1f4e4f7f205be0b4de08344a
6716a639465df352d0

[Alen = 1]

Key = 01e832095336b761d06f399b279a6d22
Nonce = 20da58d0c347574168b33c4e43

Count = 10
Adata = 95
Payload = aa2253e7e045d7ca29d7166e592f9a856f1e7b146a77d51a5ece7972c67fe3fa
CT =
f7658c566c0823b7f41a5e4cddf4d4a5e749546b3f6d2eccf6481065c2597ba2caa5a2c7843d1f
c09569a27ce465cfb9

Count = 11

```
Adata = 1e
Payload = 1446e4da336d243ee01843bc15b116a765c701a37ab00d65c1733bba64e519cb
CT =
49013b6bbf20d0433dd50b9e916a5887ed902edc2faaf6b369f552ad60c38193a163875d91e365
2b5bb3dcad97e93b61
```

```
Count = 12
Adata = 99
Payload = 307dfa454afa61b6475889b5266797254ec73358daf28430347c5b85e59aaec7
CT =
6d3a25f4c6b795cb9a95c197a2bcd905c6901c278fe87fe69cfa3292e1bc369f7975cb299dc8ef
5419e488623d86388b
```

```
.
.
.
```

B.3.2 VPT128.rsp

```
# CAVS 4.0
# "CCM-VPT" information for "CCMTest"
# AES Keylen: 128
```

```
Alen = 32
Nlen = 13
Tlen = 16
```

```
[Plen = 0]
```

```
Key = 2438b445f95ba98fdda32f25e761a5f5
Nonce = 108dce929ea09f3e77be87fe16
```

```
Count = 0
Adata = e1661ae3c88c556bc902cacab56572a5ed9d614ecbb54b3c3de947b9b301d3db
Payload = 00
CT = 9ef776fe20a953e153461f68685fd56f
```

```
Count = 1
Adata = 938b0cbcc263962a95cfdfe3ee7bf8848199568189cb2621b943e0ca76281f7f
Payload = 00
CT = 2786f31a04dfac83750cdd4dee02de8d
```

```
Count = 2
Adata = 17e20c9ea87ba1ff67d50b936fb0dd3779f42e32fe44e26a9cd52bd8bb814e39
Payload = 00
CT = d808677b9a960feac77a4afcc4901163
```

```
Count = 3
Adata = e9c6e0ec6bf76e284bdd667ed1f270c40c5a2fe7c50acf30b130ddc6eacf5c75
Payload = 00
CT = b5deaf1c2c2660448d62315614bc9c40
```

```
Count = 4
Adata = 3ae168d04cae3aea8e79611e35f8c97aaa3f45537fe42586a8610a03e8b9f98d
```

Payload = 00
CT = 2b337f5a6f4d22b08869b2ed453b144b

Count = 5
Adata = 4435620fdb8a1cb80763f166c85de1cf46615250acf16af064b8ec0a730cd7a
Payload = 00
CT = d9d047a6943a21c107119304f9538f01

Count = 6
Adata = 6bfb4fb50e51d2e1ac576096b119e7d9a35442e758d80ebe6730b9dfdc85db53
Payload = 00
CT = 1c70d0329b21ae05c1664a233dade23b

Count = 7
Adata = b4044a459bb64273157e8710386ef06d9d0808b4595ea92a2e77ccb203f59f93
Payload = 00
CT = a8e5ac484fd2ce45d6e9a15dbdbf8283

Count = 8
Adata = d65cac0355cecb8768fb4d236f96abbcc9516033eaa09c42aebf3ca7edf6fa85
Payload = 00
CT = 9f02e81c4c1e85623e94ab69734eb2e3

Count = 9
Adata = 1aa20368513bbde4177998dae53dfdd99d36efa979049f8b419d3ac1c2f00651
Payload = 00
CT = ebcc27d11c4a094e54339f974430dd21

[Plen = 1]

Key = 8ab59095b6f6c16c37a267b7dc635b80
Nonce = 0b591ac62841e5202c3e155b5c

Count = 10
Adata = ad2d96132445138743b791d154f4cb92073b14a068bcea4e0dfecded947e5292
Payload = 5c
CT = 331424d3e5f3d0dcd8bb954985e2a701e7

Count = 11
Adata = 4010296f60f3f9d9d0dadcaa327021000dbab44ccec52ffcc9986ef95ae355b
Payload = 33
CT = 5ca30976a7e77d01e8a851a27e4abef31a

Count = 12
Adata = 80fb10b3da25359e47920cfcfbf15a5149bb8731b493f34b88f18da73cbfa12c
Payload = 83
CT = ecc0d9b5e2f2ac20b700c18a0c36d16e95

.

.

.

B.3.3 VNT128.rsp

```
# CAVS 4.0
# "CCM-VNT" information for "CCMTest"
# AES Keylen: 128

Alen = 32
Plen = 32
Tlen = 16

[Nlen = 7]

Key = f53c712b9f4b5c5e6cf27ef3f8ac73ea

Count = 0
Nonce = db3e34e6404c8e
Adata = 0c7316150d38b0cf8df11c0a9dbb1078bc6b20274a2cd84b3f6a083e1cef5fc5
Payload = 0250670e86463e9dd98807d8a8e0f085aeebb8b2cdd5679f5d643dd8c438e8a2
CT =
c300313252c9073c1d6a51478ac6221d3c1292d07a5c8c6c4b57a81eea62cb7d230c0a1aa08681
a328f8708a0fa6d074

Count = 1
Nonce = ad8f2a8810023d
Adata = c3ec92aced686e68067a663aa1b7c8099ad77de64f18e0910dddd13fc99b049a
Payload = 38fda30748eabf412fba06874ae06c0dcc5752c2be92a9dd45b55bb82405e6e2
CT =
6fd70b2f43b7372c1da42788709c665e165995238693aaae29e44e8120c07dc93385afe91f8363
d1e3751195d6fd49a8

Count = 2
Nonce = 0915baald7245e
Adata = b2207f9c0f0426f171ff18b2a4392f61fb4ee4a44c476fe03dc93009be8c4eb9
Payload = 6a2f9201da0fa4f8b1962a58feaa41576f4db529b9717c733a0e8302dd73aebd
CT =
116ecedb4236068cf0f58e775770710be775d5d9091ee457df067204d053aa9e1fbb531662b3fa
a5e4f9083d704f3b69

Count = 3
Nonce = e9b76ca0f93cfb
Adata = 6c05dd99097ccb16fda6819ac39d022920a4d344635d5fbbec3c9ac3eb3be548
Payload = 965b71f155ee858955d652d693efd13cf35c27a0d4ced5cee6022f18408c0f40
CT =
e081a95a986691fa9c0dc95051a7350814e78813c18140765f2c0c6154927e900352f6ea139192
3a243746c57026f835

Count = 4
Nonce = f552bf199d0ac6
Adata = b0eb93c330a111a4b2e527fd19a06a1c46bc6964dedc8fa34e4a4b9f0d306df2
Payload = bfd1e7f5478b010a20f719f11f284186790b0630cd54987265b82bbdb95d9c89
CT =
00b1b5ea9ae7b9ebbf55f4742f9fe0c5789a3ddf821eaba2c1c1b018169241cd07d5d8bb588129
d7439ccda3596e4bd1
```

Count = 5
Nonce = 46dc5c84c5c3b1
Adata = e9d74e527a15fff43e276570b5ad70e91046cdcc2e4b396282ba69bbfbc356e05
Payload = e85bb8b3fc20aa5cc0dbaa0aeeebec30fd7d3981a200930598d91c6d9d5834a4
CT =
c6af9e02df383b29a6f634b0c501e1e92c1001282c557b1d8150e8e104d2e906059602aff5bd28
efb401ae8222e91780

Count = 6
Nonce = ec84e37cfe420c
Adata = 42a4c249ff283c068c7d8e5ed5eab2f64149e5a79560ab73156f13beec063cba
Payload = 12a3d7b4227c6fbecf5196969a3368fd11068719963405c462a3842acae49b93
CT =
287a20ddee78a2e898b80244540a68ab48f994ea7df5fa7e584fd6d4572cdc70c0e72ad230bce6
15eb36bf7895a5db68

Count = 7
Nonce = 20809dfd638e24
Adata = 4f5331899a4cf958fb0099819ef94302da469b8011cdbc39d8e37b3a581aefd2
Payload = 150133285890c10c4541886d3f3c1e5ca2bbe287fa6ed8b8731fb49e919234d0
CT =
b3f483e32a60f8e78311d860f017509c60d128c317952171697e19115afb311caa6d64d375621c
a58957e1f546086a20

Count = 8
Nonce = 17c329e64cf55c
Adata = 5752565d411ca6a6fd67860041e57540a1a4d391a9d8985f29db4574d0721b61
Payload = 0ea808ce758a65f491ca2185d171385c35cdcce6035c762abcecd064eff7ebb
CT =
0dd33d4a13e2952c838d1aeaf3c4301339408e059b83820622d125823cd93e7de42adff61fd84e
1ebbef01daa1b7df85

Count = 9
Nonce = 77279387f30a1f
Adata = f38ce2ed5868711988f2c49209eaa8be378e756b36be9c122b5e805dacfc87e6
Payload = 4ad33e1b998b6014d0c4614db0c5bc67245f4ae28123aeea0cd2f074bd15688a
CT =
a2e54c80610d9d3e2dc92eb6ab3d0633bad5cde39df576c1aeld9a48de01fc37667c6046d9ae47
6010e1891d5b3c27d3

[Nlen = 8]

Key = f0bc7ebd9f8ac31a42b646be0a78eb4f

Count = 10
Nonce = 1b587128ad11400e
Adata = 3029db22aba5ebab2053f39b7b07c97de7cba2c5d9d3326451af149a5dc46b0b
Payload = 7d3098cb1fc5a1954aea7d5b2ede03e38839fa2a75728b0288a4f5ff1a928394
CT =
2221c311f7bba4eed9aa83caceafcf6e4e5f641f20ae2217232c0e51f851d19549bb1b4e0f122
affe20e2324fe0e7fd

Count = 11

```
Nonce = c3be3ba92028b748
Adata = f2448f99a631ee4a6c95e154ea8de0dcfc97446c56a407a46b6fcc2d8e0c1fef
Payload = 859157f53a401a7a8706044aa24e9e64e2259743240351556de8a0afd1abceff
CT =
e23efbc1040d85d2d2227626e44ebcc296f372d1b5bb89a904789c51f4abf72ca5cc836041abd8
99b64f8b7db9323aa8
```

```
Count = 12
Nonce = 093983c684e75dcb
Adata = 550cfc1e529b013fa8b5a5bd2c67122df500ab771cc5f029c0e6a2114db1280a
Payload = 580bbe3260a80738ee5b12e6b2e727b8464bdb40064484c82213f039f280573b
CT =
27e04d474cd9d46b854851656c0925ce9d91e825d636254e4d81bc2210818017852c2be0f32775
2f0b784fb205898afd
```

```
.
.
.
```

B.3.4 VTT128.rsp

```
# CAVS 4.0
# "CCM-VTT" information for "CCMTest"
# AES Keylen: 128
```

```
Alen = 32
Plen = 32
Nlen = 13
```

```
[Tlen = 4]
```

```
Key = 0ca55a6d8e5104a586c5d00b364fa187
Nonce = 8b2f2d20703538ea929312bb3e
```

```
Count = 0
Adata = 89182405c706aacab3cbf8425fc745dd4ffdd3e07d0c17ffa0621a2daeac1fb3
Payload = b6fa778f4bfc6dfe4d4aca505d4b6bbf57c413d23cf903977015cb2d26cb5f86
CT = 5faa490e44a1e88989b329ae87f215255b46450642fc779eac2d8b0220a65b84f011348a
```

```
Count = 1
Adata = fadf339fd4bd94c5c1147a97026e5399981c3d3fb4d71cb36fa7e9d2bb044d77
Payload = 23f8fb9b2cdaa10715e08b94d0c5dbea3b7ffbdea2ba3b8d8584bca79c4a8e0e
CT = caa8c51a23872470d119686a0a7ca57037fdad0adcbf4f8459bcfc889a278a0c7962dcdbd
```

```
Count = 2
Adata = e66a77b24b5899c8d2a356fd36acd7df9d940fac1aac5668762d532c302a20c1
Payload = 536fd560b83ac5dd9bc3d205786a66e73741e1b648cc46b8f205345ee8a319b5
CT = ba3febelb76740aa5f3a31fba2d3187d3bc3b76236c932b12e3d7471eece1db775651fe4
```

```
Count = 3
Adata = d23093e1c5258caf72151a2dbe206b245a03d9d5989a62977ea358c11ac459ca
Payload = e6184bc8c178alaba852a239941027b15788b84dd2695dc669d9b21bb45c3a8f
CT = 0f487549ce2524dc6cab41c74ea9592b5b0aee99ac6c29cfb5e1f234b2313e8d81911408
```

Count = 4
Adata = 49fafa6fa7685b8ebd09090fe0f396c5e4b623e28431dd6a03abc8e7141fbc5f
Payload = a5df31a9a76e0ad25429c900ca0f87b901812d1545eb877deaa69ab33b1d3812
CT = 4c8f0f28a8338fa590d02afe10b6f9230d037bc13beef374369eda9c3d703c10ee97a2a5

Count = 5
Adata = 333711870519a55637e750537f8f1803a1d8758490f4a0c3d6580def37cb362d
Payload = ce7877b9a86a67d6c3fb4aaa17d86b5fedb3035ce6385dd14043388f55506d1e
CT = 27284938a737e2a10702a954cd6115c5e1315588983d29d89c7b78a0533d691c6db2f4ca

Count = 6
Adata = 0e2885db43bb745831059c13aae17969282e82c0052c010fee2923a2955e4b17
Payload = c21454e083330abb387f22c2790306051fff87659debceb194b8950fa159979e
CT = 2b446a618c6e8fccfc86c13ca3ba789f137dd1b1e3eebab84880d520a734939c23015a32

Count = 7
Adata = ed4db3dd7fab9e52bc636e3b37887bdb3d039c0369d9537a73ac44a14985ec57
Payload = bde29a2eab396e652f74a73a70ad49b03a12178ffdddb400198608575836e530
CT = 54b2a4afa464eb12eb8d44c4aa14372a3690415b83d8c009c5be48785e5be1321ad451e8

Count = 8
Adata = 80f8235f264c99e80968348b040ebdbe430be04bf71682544efc5495a2faa8ea
Payload = de182cda7c44d5966476be9f4043755baa69158937bd6ad5b46555a9af477247
CT = 3748125b731950e1a08f5d619afa0bc1a6eb435d49b81edc685d1586a92a764501cab1d1

Count = 9
Adata = d8cb7cb847410e6a3f78502d9ea0483ec07b362c07acca3bbb3295061530be69
Payload = 8f45f26fa0822c2a73428697fa7e9c30da17626cc2d315e0fba271aa4127250f
CT = 6615cceeafdfa95db7bb656920c7e2aad69534b8bcd661e9279a3185474a210d329b27f6

[Tlen = 6]

Key = 3619dd376a7902385531b5d0b9c6f458
Nonce = 200e953c0616887f2832f24be7

Count = 10
Adata = 270338ecc3987e4a64cbe751c96ec4a06539c5b905d5bcb3b433a530db22e48f
Payload = 987d0205bdffea464c978e4f8ffa2491fe4e898304df27f506131ca2a2a09904
CT =
5f3c0e7c4cf305756c93783cbfe31f0c6fa56a325c37bf2b7b9571c51caa7124351942e7d253

Count = 11
Adata = 21b788ca8e96b71d3ecd78de27ca96837a4be65dd6c41d19bb00e48d410a2fb2
Payload = ddaff7d549344f595c5df062bffd2f8650df7881df45e426306b9bf7c4a81e7
CT =
1aeefbacb838a06a7c5906118fe4c965f4e61439451cc69c1e80d4d8c24069c76b57cc5b2541

Count = 12
Adata = 9dabcf6f967c6ca60c0e1ca329b27be58968171049a625d76154731e341b9e60
Payload = 903b2599d8b7f78eefcedd9cc8797b2259a49e09f1332deecc435d83e5b22332
CT =
577a29e029bb18bdcfca2beff86040bfc84f7db8a9dbb530b1c530e45bb8cb12f3eb94386919

.
.

B.3.5 DVPT128.rsp

```
# CAVS 4.0
# "CCM-DVPT" information for "CCMTest"
# AES Keylen: 128
```

```
[Alen = 0, Plen = 0, Nlen = 7, Tlen = 4]
```

```
Key = 0cb1e2654c33da429ebef20b53b121a8
```

```
Count = 0
Nonce = afe6f12d0ea174
Adata = 00
Payload = 00
CT = ab72b36b
Result = Pass
```

```
Count = 1
Nonce = da7dfe30a59977
Adata = 00
Payload = 00
CT = 5de8d3e2
Result = Fail
```

```
Count = 2
Nonce = 753ded3501a6ca
Adata = 00
Payload = 00
CT = a44784a4
Result = Pass
```

```
Count = 3
Nonce = 49a7e02c8f0186
Adata = 00
Payload = 00
CT = 0d1331c9
Result = Fail
```

```
Count = 4
Nonce = 688a92a78e57b2
Adata = 00
Payload = 00
CT = dd507b85
Result = Pass
```

```
Count = 5
Nonce = 8c84018b595ff1
Adata = 00
Payload = 00
CT = b49eb878
```

Result = Fail

Count = 6
Nonce = f06f3e1b1428e5
Adata = 00
Payload = 00
CT = c5d14a98
Result = Fail

Count = 7
Nonce = b5430fb552c2cc
Adata = 00
Payload = 00
CT = 7419968c
Result = Fail

Count = 8
Nonce = 87e3324b5fb4f5
Adata = 00
Payload = 00
CT = c40e6e92
Result = Fail

Count = 9
Nonce = a3ac390add8073
Adata = 00
Payload = 00
CT = 84fe8dd3
Result = Pass

Count = 10
Nonce = ae69674ea08a60
Adata = 00
Payload = 00
CT = 4e021854
Result = Pass

Count = 11
Nonce = ae4d72eaf8dcb7
Adata = 00
Payload = 00
CT = acc80bca
Result = Fail

Count = 12
Nonce = 9c42a04aeb5b86
Adata = 00
Payload = 00
CT = c6458ec7
Result = Fail

Count = 13
Nonce = 594b76db2d290e
Adata = 00

Payload = 00
CT = 2ed90865
Result = Fail

Count = 14
Nonce = 709e122f1d714c
Adata = 00
Payload = 00
CT = c0610700
Result = Fail

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 16]

Key = 50de369adcba6018a7c9214de0cf3ac1

Count = 15
Nonce = afe6f12d0ea174
Adata = 00
Payload = 00
CT = 1610970994a785163d128b22cf21d535
Result = Pass

Count = 16
Nonce = da7dfe30a59977
Adata = 00
Payload = 00
CT = 941bd3b74ceaf849d39bdd29b8fb0869
Result = Fail

Count = 17
Nonce = 753ded3501a6ca
Adata = 00
Payload = 00
CT = dc2c46d367f346977602bff216097b47
Result = Pass

.
. .
.

B.4 Example of the *SAMPLE* File

B.4.1 VADT128.sam

```
# CAVS 4.0  
# "CCM-VADT" information for "CCMTest"  
# AES Keylen: 128  
# Generated on Thu Jul 29 08:03:51 2004
```

Plen = 32
Nlen = 13
Tlen = 16

[Alen = 0]

Key = 3751c2240d92f4ecdbf5a7824f3d1e6d
Nonce = 92f0935f0e3abc1793e25da5d4

Count = 0
Adata = 00
Payload = 235a8a308fa82bebc614fc79510e7df0456afee923b6a979fdcabc363daa22f8b
CT = ?

Count = 1
Adata = 00
Payload = 47c12148eedaeceb3b90350740ba4f357fe3648a0ae4b7c9e8b92bd6bb8d096e
CT = ?

Count = 2
Adata = 00
Payload = cf54a7b373b8c7b39915853afb4b124cdd9e6f73f00c74b575dd17c3a57deb73
CT = ?

Count = 3
Adata = 00
Payload = 4b5b55d828212b1e3f6310a738f81593c88eb9b386375c36fa24f685f7af086b
CT = ?

Count = 4
Adata = 00
Payload = 259ff0308e071104a5460647b6c7a73f7ab188024653cdf083c53f815ecc9f41
CT = ?

Count = 5
Adata = 00
Payload = 15b201539166a657e29bd6a5a77ed3feec01950b0631cd4ebdc52459b1f2c33e
CT = ?

Count = 6
Adata = 00
Payload = 9552e3087f164bf58bbc3cb3db699ba3209e347518ae593d5576ccc93f48e032
CT = ?

Count = 7
Adata = 00
Payload = d760547fd96a4b9eb47695b9bb98c3aab09f40c6e5a28f10a2dbd4adc7b89698
CT = ?

Count = 8
Adata = 00
Payload = 502a753b671d3e3d8785e7de14cc84ed705d254fbf59b64dee8c2432f39fc216
CT = ?

Count = 9
Adata = 00
Payload = 3783067c8eab48c2d4c95b82e9d2af7d54b9b865d1e594f209e2ee32a0572221
CT = ?

[Alen = 1]

Key = 01e832095336b761d06f399b279a6d22
Nonce = 20da58d0c347574168b33c4e43

Count = 10
Adata = 95
Payload = aa2253e7e045d7ca29d7166e592f9a856f1e7b146a77d51a5ece7972c67fe3fa
CT = ?

Count = 11
Adata = 1e
Payload = 1446e4da336d243ee01843bc15b116a765c701a37ab00d65c1733bba64e519cb
CT = ?

Count = 12
Adata = 99
Payload = 307dfa454afa61b6475889b5266797254ec73358daf28430347c5b85e59aaec7
CT = ?

.
. .
.

B.4.2 VPT128.sam

```
# CAVS 4.0  
# "CCM-VPT" information for "CCMTest"  
# AES Keylen: 128  
# Generated on Thu Jul 29 08:03:52 2004
```

Alen = 32
Nlen = 13
Tlen = 16

[Plen = 0]

Key = 2438b445f95ba98fdda32f25e761a5f5
Nonce = 108dce929ea09f3e77be87fe16

Count = 0
Adata = e1661ae3c88c556bc902cacab56572a5ed9d614ecbb54b3c3de947b9b301d3db
Payload = 00
CT = ?

Count = 1
Adata = 938b0cbcc263962a95cfdfe3ee7bf8848199568189cb2621b943e0ca76281f7f
Payload = 00
CT = ?

Count = 2
Adata = 17e20c9ea87ba1ff67d50b936fb0dd3779f42e32fe44e26a9cd52bd8bb814e39
Payload = 00
CT = ?

Count = 3
Adata = e9c6e0ec6bf76e284bdd667ed1f270c40c5a2fe7c50acf30b130ddc6eacf5c75
Payload = 00
CT = ?

Count = 4
Adata = 3ae168d04cae3aea8e79611e35f8c97aaa3f45537fe42586a8610a03e8b9f98d
Payload = 00
CT = ?

Count = 5
Adata = 4435620fdb8a1cb80763f166c85de1cf46615250acf16af064b8ec0a730cd7a
Payload = 00
CT = ?

Count = 6
Adata = 6bfb4fb50e51d2e1ac576096b119e7d9a35442e758d80ebe6730b9dfdc85db53
Payload = 00
CT = ?

Count = 7
Adata = b4044a459bb64273157e8710386ef06d9d0808b4595ea92a2e77ccb203f59f93
Payload = 00
CT = ?

Count = 8
Adata = d65cac0355cecb8768fb4d236f96abbcc9516033eaa09c42aebf3ca7edf6fa85
Payload = 00
CT = ?

Count = 9
Adata = 1aa20368513bbde4177998dae53dfdd99d36efa979049f8b419d3ac1c2f00651
Payload = 00
CT = ?

[Plen = 1]

Key = 8ab59095b6f6c16c37a267b7dc635b80
Nonce = 0b591ac62841e5202c3e155b5c

Count = 10
Adata = ad2d96132445138743b791d154f4cb92073b14a068bcea4e0dfecded947e5292
Payload = 5c
CT = ?

Count = 11
Adata = 4010296f60f3f9d9d0dadcaa3270210000dbab44ccec52ffcc9986ef95ae355b
Payload = 33
CT = ?

Count = 12
Adata = 80fb10b3da25359e47920cfcbfb15a5149bb8731b493f34b88f18da73cbfa12c
Payload = 83

CT = ?

.
. .
.

B.4.3 VNT128.sam

```
# CAVS 4.0
# "CCM-VNT" information for "CCMTest"
# AES Keylen: 128
# Generated on Thu Jul 29 08:03:52 2004
```

```
Alen = 32
Plen = 32
Tlen = 16
```

```
[Nlen = 7]
```

```
Key = f53c712b9f4b5c5e6cf27ef3f8ac73ea
```

```
Count = 0
Nonce = db3e34e6404c8e
Adata = 0c7316150d38b0cf8df11c0a9dbb1078bc6b20274a2cd84b3f6a083e1cef5fc5
Payload = 0250670e86463e9dd98807d8a8e0f085aeebb8b2cdd5679f5d643dd8c438e8a2
CT = ?
```

```
Count = 1
Nonce = ad8f2a8810023d
Adata = c3ec92aced686e68067a663aa1b7c8099ad77de64f18e0910dddd13fc99b049a
Payload = 38fda30748eabf412fba06874ae06c0dcc5752c2be92a9dd45b55bb82405e6e2
CT = ?
```

```
Count = 2
Nonce = 0915baald7245e
Adata = b2207f9c0f0426f171ff18b2a4392f61fb4ee4a44c476fe03dc93009be8c4eb9
Payload = 6a2f9201da0fa4f8b1962a58feaa41576f4db529b9717c733a0e8302dd73aebd
CT = ?
```

```
Count = 3
Nonce = e9b76ca0f93cfb
Adata = 6c05dd99097ccb16fda6819ac39d022920a4d344635d5fbbec3c9ac3eb3be548
Payload = 965b71f155ee858955d652d693efd13cf35c27a0d4ced5cee6022f18408c0f40
CT = ?
```

```
Count = 4
Nonce = f552bf199d0ac6
Adata = b0eb93c330a111a4b2e527fd19a06a1c46bc6964dedc8fa34e4a4b9f0d306df2
Payload = bfd1e7f5478b010a20f719f11f284186790b0630cd54987265b82bbdb95d9c89
CT = ?
```

```
Count = 5
Nonce = 46dc5c84c5c3b1
Adata = e9d74e527a15ff43e276570b5ad70e91046cdcc2e4b396282ba69bbfbc356e05
```

Payload = e85bb8b3fc20aa5cc0dbaa0aeeebec30fd7d3981a200930598d91c6d9d5834a4
CT = ?

Count = 6
Nonce = ec84e37cfe420c
Adata = 42a4c249ff283c068c7d8e5ed5eab2f64149e5a79560ab73156f13beec063cba
Payload = 12a3d7b4227c6fbecf5196969a3368fd11068719963405c462a3842acae49b93
CT = ?

Count = 7
Nonce = 20809dfd638e24
Adata = 4f5331899a4cf958fb0099819ef94302da469b8011cdbc39d8e37b3a581aefd2
Payload = 150133285890c10c4541886d3f3c1e5ca2bbe287fa6ed8b8731fb49e919234d0
CT = ?

Count = 8
Nonce = 17c329e64cf55c
Adata = 5752565d411ca6a6fd67860041e57540a1a4d391a9d8985f29db4574d0721b61
Payload = 0ea808ce758a65f491ca2185d171385c35cdcce6035c762abcecd064eff7ebb
CT = ?

Count = 9
Nonce = 77279387f30a1f
Adata = f38ce2ed5868711988f2c49209eaa8be378e756b36be9c122b5e805dacfc87e6
Payload = 4ad33e1b998b6014d0c4614db0c5bc67245f4ae28123aeea0cd2f074bd15688a
CT = ?

[Nlen = 8]

Key = f0bc7ebd9f8ac31a42b646be0a78eb4f

Count = 10
Nonce = 1b587128ad11400e
Adata = 3029db22aba5ebab2053f39b7b07c97de7cba2c5d9d3326451af149a5dc46b0b
Payload = 7d3098cb1fc5a1954aea7d5b2ede03e38839fa2a75728b0288a4f5ff1a928394
CT = ?

Count = 11
Nonce = c3be3ba92028b748
Adata = f2448f99a631ee4a6c95e154ea8de0dcfc97446c56a407a46b6fcc2d8e0c1fef
Payload = 859157f53a401a7a8706044aa24e9e64e2259743240351556de8a0afd1abcefff
CT = ?

Count = 12
Nonce = 093983c684e75dcb
Adata = 550cfc1e529b013fa8b5a5bd2c67122df500ab771cc5f029c0e6a2114db1280a
Payload = 580bbe3260a80738ee5b12e6b2e727b8464bdb40064484c82213f039f280573b
CT = ?

.
. .
.

B.4.4 VTT128.sam

```
# CAVS 4.0
# "CCM-VTT" information for "CCMTest"
# AES Keylen: 128
# Generated on Thu Jul 29 08:03:52 2004

Alen = 32
Plen = 32
Nlen = 13

[Tlen = 4]

Key = 0ca55a6d8e5104a586c5d00b364fa187
Nonce = 8b2f2d20703538ea929312bb3e

Count = 0
Adata = 89182405c706aacab3cbf8425fc745dd4ffdd3e07d0c17ffa0621a2daeac1fb3
Payload = b6fa778f4bfc6dfe4d4aca505d4b6bbf57c413d23cf903977015cb2d26cb5f86
CT = ?

Count = 1
Adata = fadf339fd4bd94c5c1147a97026e5399981c3d3fb4d71cb36fa7e9d2bb044d77
Payload = 23f8fb9b2cdaa10715e08b94d0c5dbea3b7ffbdea2ba3b8d8584bca79c4a8e0e
CT = ?

Count = 2
Adata = e66a77b24b5899c8d2a356fd36acd7df9d940fac1aac5668762d532c302a20c1
Payload = 536fd560b83ac5dd9bc3d205786a66e73741e1b648cc46b8f205345ee8a319b5
CT = ?

Count = 3
Adata = d23093e1c5258caf72151a2dbe206b245a03d9d5989a62977ea358c11ac459ca
Payload = e6184bc8c178a1aba852a239941027b15788b84dd2695dc669d9b21bb45c3a8f
CT = ?

Count = 4
Adata = 49fafa6fa7685b8ebd09090fe0f396c5e4b623e28431dd6a03abc8e7141fbc5f
Payload = a5df31a9a76e0ad25429c900ca0f87b901812d1545eb877deaa69ab33b1d3812
CT = ?

Count = 5
Adata = 333711870519a55637e750537f8f1803a1d8758490f4a0c3d6580def37cb362d
Payload = ce7877b9a86a67d6c3fb4aaa17d86b5fedb3035ce6385dd14043388f55506d1e
CT = ?

Count = 6
Adata = 0e2885db43bb745831059c13aae17969282e82c0052c010fee2923a2955e4b17
Payload = c21454e083330abb387f22c2790306051fff87659debceb194b8950fa159979e
CT = ?

Count = 7
Adata = ed4db3dd7fab9e52bc636e3b37887bdb3d039c0369d9537a73ac44a14985ec57
```

Payload = bde29a2eab396e652f74a73a70ad49b03a12178ffdddb400198608575836e530
CT = ?

Count = 8
Adata = 80f8235f264c99e80968348b040ebdbe430be04bf71682544efc5495a2faa8ea
Payload = de182cda7c44d5966476be9f4043755baa69158937bd6ad5b46555a9af477247
CT = ?

Count = 9
Adata = d8cb7cb847410e6a3f78502d9ea0483ec07b362c07acca3bbb3295061530be69
Payload = 8f45f26fa0822c2a73428697fa7e9c30da17626cc2d315e0fba271aa4127250f
CT = ?

[Tlen = 6]

Key = 3619dd376a7902385531b5d0b9c6f458
Nonce = 200e953c0616887f2832f24be7

Count = 10
Adata = 270338ecc3987e4a64cbe751c96ec4a06539c5b905d5bcb3b433a530db22e48f
Payload = 987d0205bdfcfea464c978e4f8ffa2491fe4e898304df27f506131ca2a2a09904
CT = ?

Count = 11
Adata = 21b788ca8e96b71d3ecd78de27ca96837a4be65dd6c41d19bb00e48d410a2fb2
Payload = ddaff7d549344f595c5df062bffd2f8650df7881df45e426306b9bf7c4a81e7
CT = ?

Count = 12
Adata = 9dabcf6f967c6ca60c0e1ca329b27be58968171049a625d76154731e341b9e60
Payload = 903b2599d8b7f78eefcedd9cc8797b2259a49e09f1332deecc435d83e5b22332
CT = ?

.
. .
.

B.4.5 DVPT128.sam

```
# CAVS 4.0  
# "CCM-DVPT" information for "CCMTest"  
# AES Keylen: 128  
# Generated on Thu Jul 29 08:03:52 2004
```

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 4]

Key = 0cb1e2654c33da429ebef20b53b121a8

Count = 0
Nonce = afe6f12d0ea174
Adata = 00
Payload = 00
CT = ab72b36b

Result = ?

Count = 1
Nonce = da7dfe30a59977
Adata = 00
Payload = 00
CT = 5de8d3e2
Result = ?

Count = 2
Nonce = 753ded3501a6ca
Adata = 00
Payload = 00
CT = a44784a4
Result = ?

Count = 3
Nonce = 49a7e02c8f0186
Adata = 00
Payload = 00
CT = 0d1331c9
Result = ?

Count = 4
Nonce = 688a92a78e57b2
Adata = 00
Payload = 00
CT = dd507b85
Result = ?

Count = 5
Nonce = 8c84018b595ff1
Adata = 00
Payload = 00
CT = b49eb878
Result = ?

Count = 6
Nonce = f06f3e1b1428e5
Adata = 00
Payload = 00
CT = c5d14a98
Result = ?

Count = 7
Nonce = b5430fb552c2cc
Adata = 00
Payload = 00
CT = 7419968c
Result = ?

Count = 8
Nonce = 87e3324b5fb4f5
Adata = 00

Payload = 00
CT = c40e6e92
Result = ?

Count = 9
Nonce = a3ac390add8073
Adata = 00
Payload = 00
CT = 84fe8dd3
Result = ?

Count = 10
Nonce = ae69674ea08a60
Adata = 00
Payload = 00
CT = 4e021854
Result = ?

Count = 11
Nonce = ae4d72eaf8dcb7
Adata = 00
Payload = 00
CT = acc80bca
Result = ?

Count = 12
Nonce = 9c42a04aeb5b86
Adata = 00
Payload = 00
CT = c6458ec7
Result = ?

Count = 13
Nonce = 594b76db2d290e
Adata = 00
Payload = 00
CT = 2ed90865
Result = ?

Count = 14
Nonce = 709e122f1d714c
Adata = 00
Payload = 00
CT = c0610700
Result = ?

[Alen = 0, Plen = 0, Nlen = 7, Tlen = 16]

Key = 50de369adcba6018a7c9214de0cf3ac1

Count = 15
Nonce = afe6f12d0ea174
Adata = 00
Payload = 00

CT = 1610970994a785163d128b22cf21d535
Result = ?

Count = 16
Nonce = da7dfe30a59977
Adata = 00
Payload = 00
CT = 941bd3b74ceaf849d39bdd29b8fb0869
Result = ?

Count = 17
Nonce = 753ded3501a6ca
Adata = 00
Payload = 00
CT = dc2c46d367f346977602bff216097b47
Result = ?

.
. .
.